2009-10-29

Aligning Security with Usability

Garfinkel, Simson

Monterey, California. Naval Postgraduate School

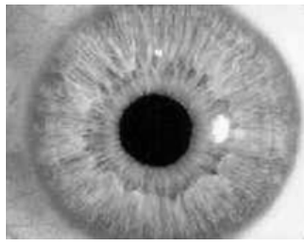
Aligning Security with Usability

Simson Garfinkel & Chris Eagle
Naval Postgraduate School

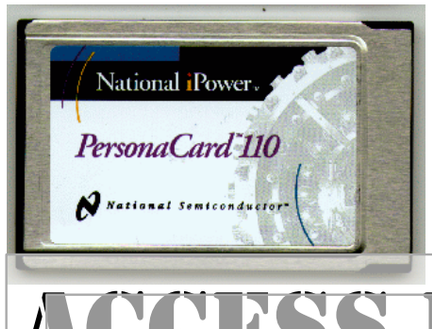
29 OCT 2009

Given the choice, which would you use...

A system that is secure but not usable.



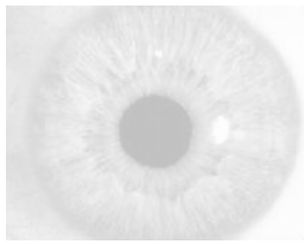
Username: simsong
Password: ••••••



ACCESS DENIED
ACCESS DENIED
ACCESS DENIED

Given the choice, which would you use...

A system that is secure but not usable.

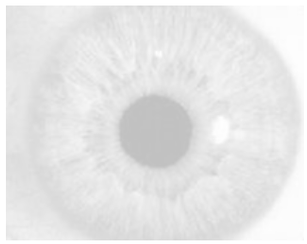


Username: simsong
Password: ••••••

ACCESS DENIED
ACCESS DENIED
ACCESS DENIED

Given the choice, which would you use...

A system that is secure but not usable.



Username: simsong
Password: ••••••

ACCESS DENIED
ACCESS DENIED
ACCESS DENIED

A system that is usable but not secure:

facebook

Sign Up

Google™

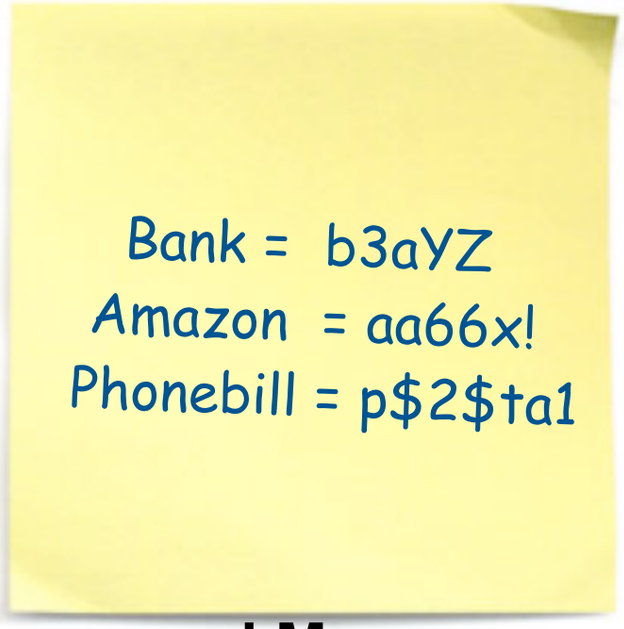
YouTube
Broadcast Yourself ™

Usability trumps security.

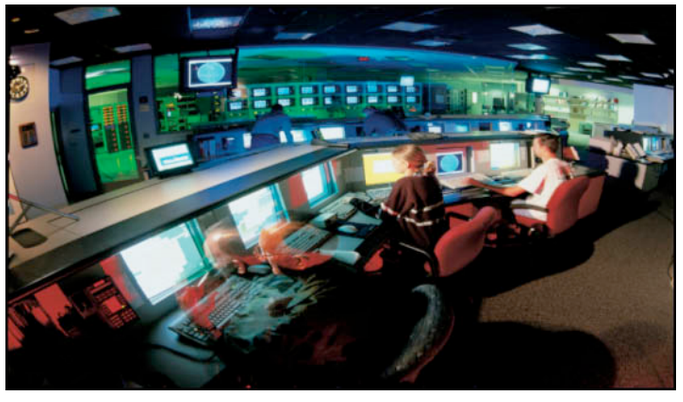
Many of today's security problems result from poor usability.

Phishing

Botnets



Password Management



Network monitoring

Aligning security and usability is a recognized priority.

2003 — Computing Research Association

- Identifies HCI-SEC as a "Grand Challenge."

2005 — President's Information Technology Advisory Committee

- "Software usability itself is a legitimate and important research topic in cyber security."

2005 — Symposium on Usable Privacy and Security founded

30 years ago, Saltzer & Schroeder identified key requirements for building secure systems.

1. Economy of mechanism.
2. Fail-safe defaults.
3. Complete mediation.
4. Open design.
5. Separation of privilege.
6. Least privilege.
7. Least common mechanism.
8. Psychological acceptability.

"The Protection of Information in Computer Systems,"
Saltzer & Schroeder, 1975

Two of these principles involve usability.

Fail-safe defaults

- “Base access decisions on permission rather than exclusion.”
- Make the system secure by default.
- [Implies control of user-initiated configuration changes.]

Psychological acceptability

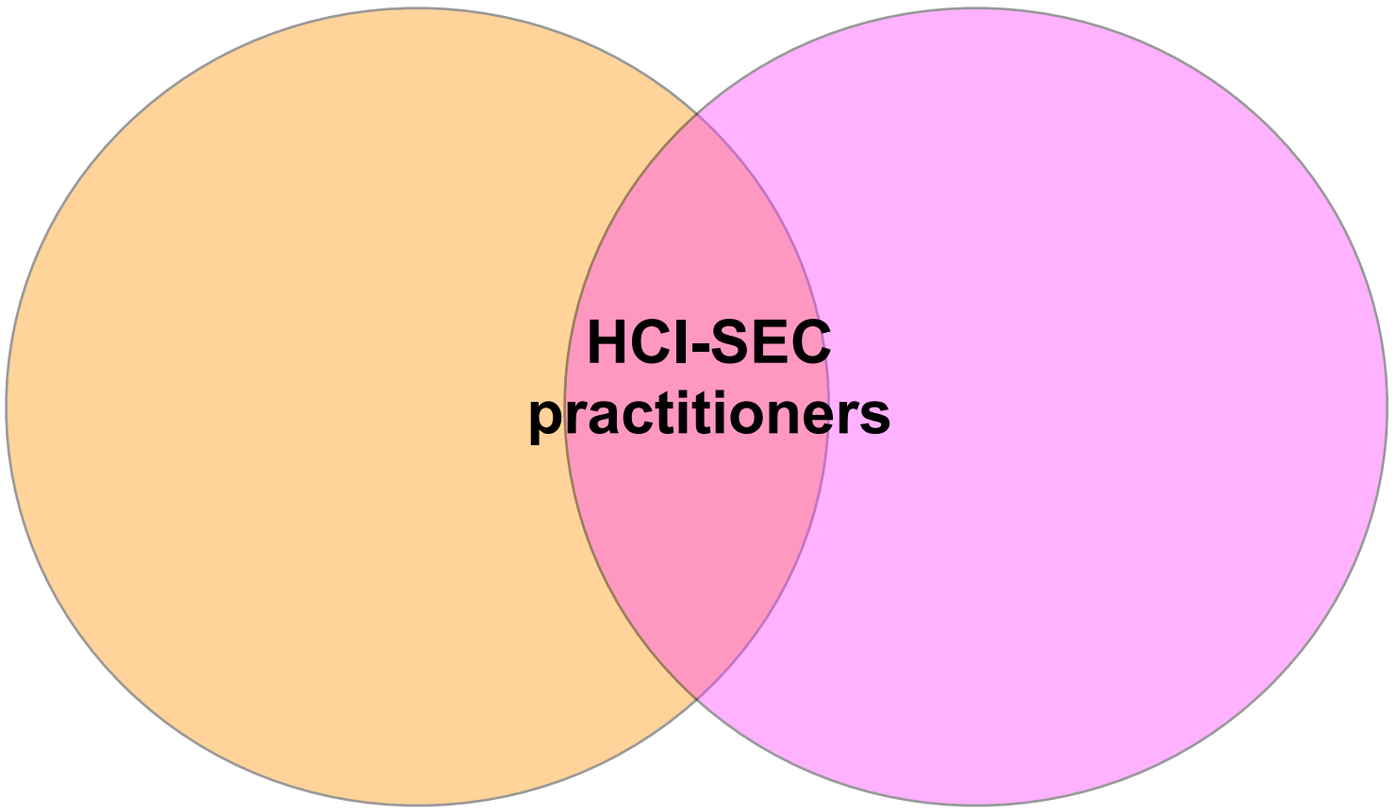
- “It is essential that the human interface be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly.”
- If the security system is not easy to use, people will circumvent it.

Why is HCI-SEC hard?

User interfaces are hard to design.

Security is hard to understand.

There just aren't that many people with both skills.

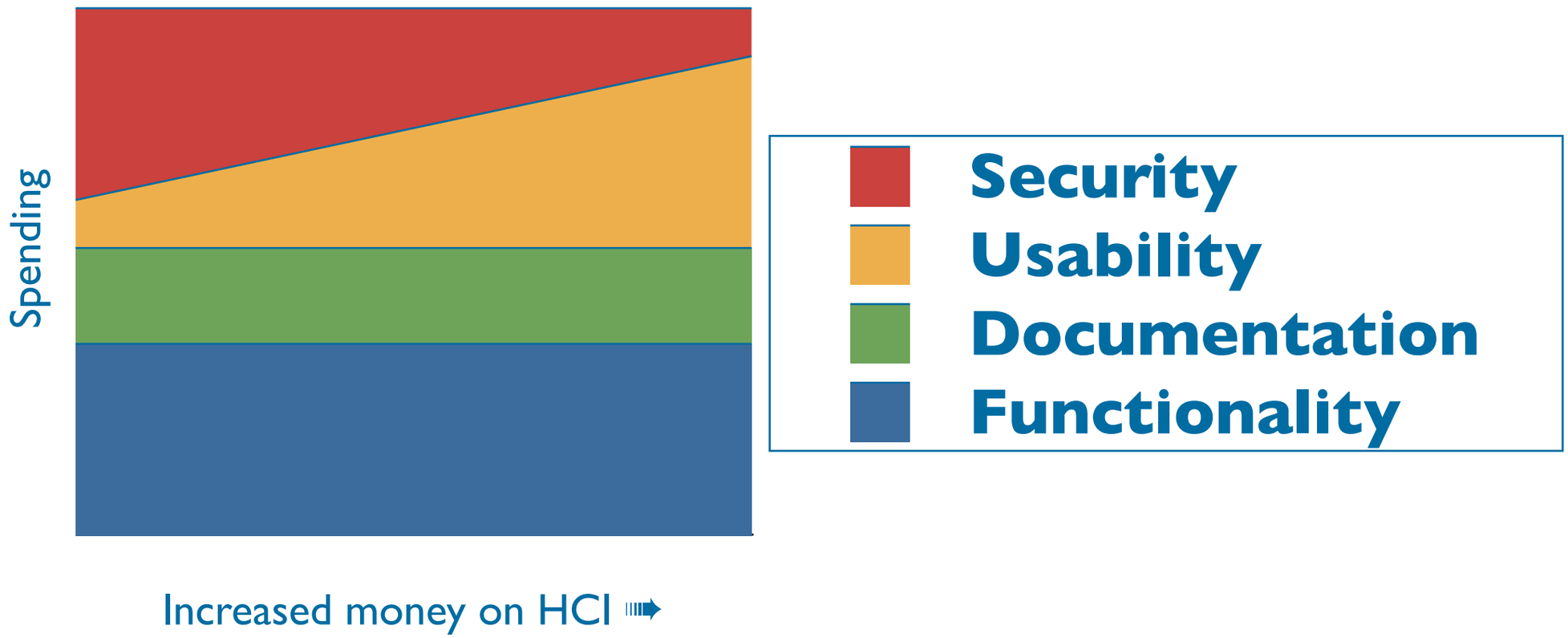


Is something else going on as well?

Security and Usability are often presented om conflict.

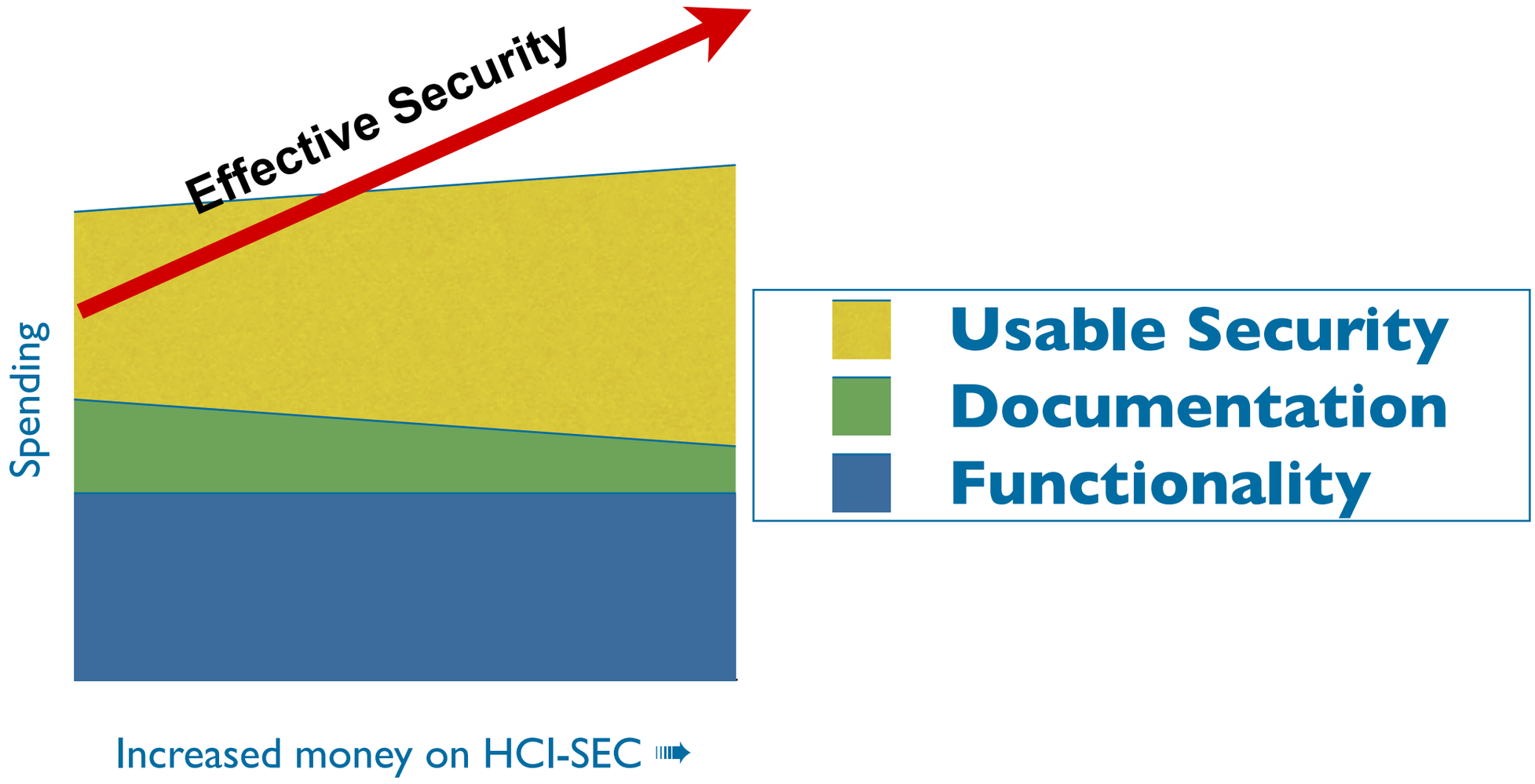
The more money spent on usability, the less available for security

```
Total cost = [Security Costs] + [Usability Costs]
                              + [Documentation Costs] + [Marketing Costs]
                              + [Functionality Costs]
```



But Security and Usability are aligned...

Increased money spent on usability can *increase* overall security



HCI-SEC

is especially hard

HCI-SEC: Usability in the face of an adversary

The adversary can exploit usability features.

The adversary can exploit usability problems.

The adversary can masquerade as tech support.

Security features make systems harder to use—so people disable them.

Adversaries adapt faster than legitimate users.

People can't distinguish attacks from system errors.

Security professionals traditionally blamed users (and administrators!)

Users are expected to:

- Use passwords that were too difficult to guess, but could be remembered without writing them down.

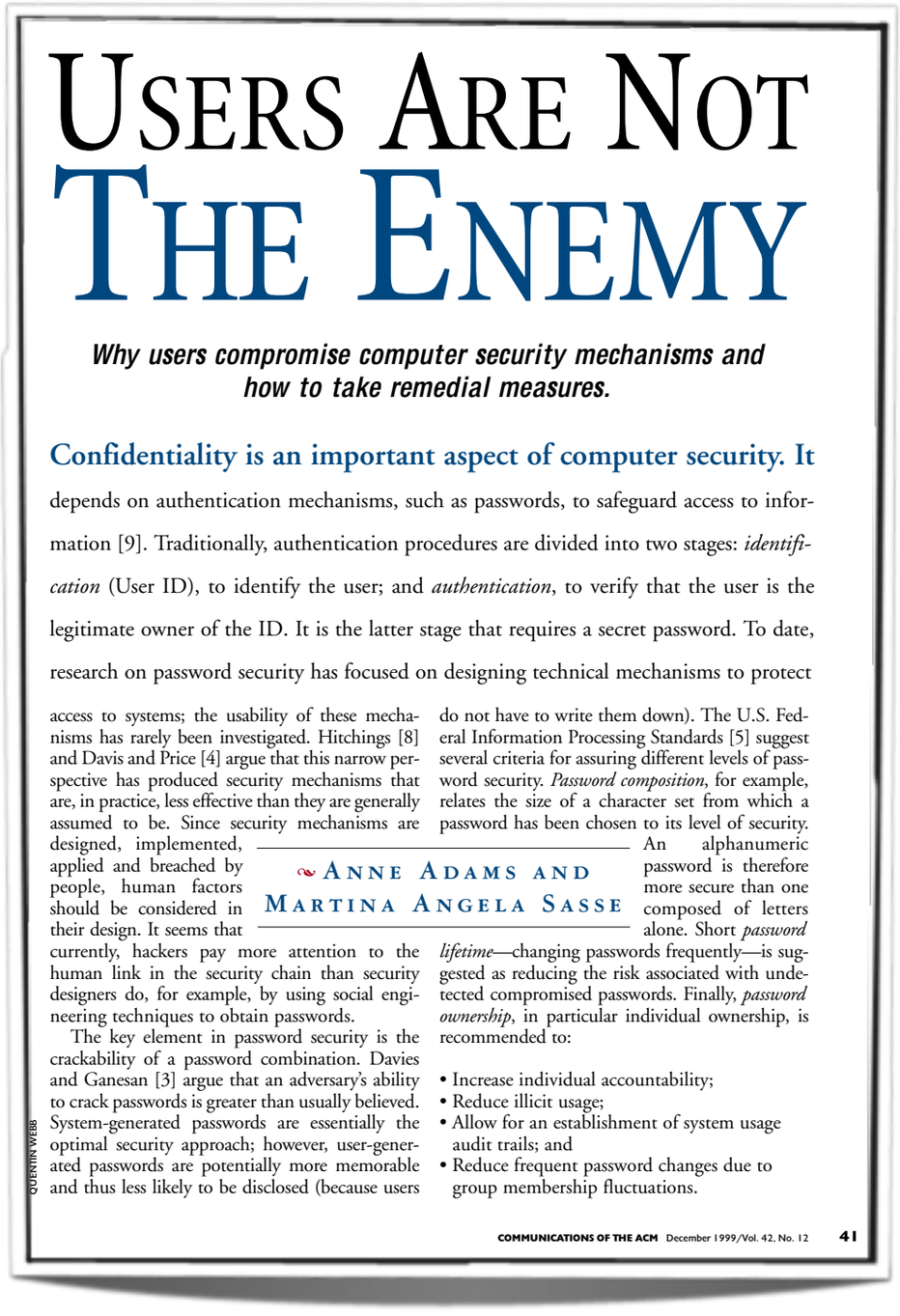
Administrators are expected to:

- Maintain system & apply patches

Developers are expected to:

- Securely code.
- Understand crypto.

Like blaming plane crashes on "pilot error."



USERS ARE NOT THE ENEMY

Why users compromise computer security mechanisms and how to take remedial measures.

Confidentiality is an important aspect of computer security. It depends on authentication mechanisms, such as passwords, to safeguard access to information [9]. Traditionally, authentication procedures are divided into two stages: *identification* (User ID), to identify the user; and *authentication*, to verify that the user is the legitimate owner of the ID. It is the latter stage that requires a secret password. To date, research on password security has focused on designing technical mechanisms to protect access to systems; the usability of these mechanisms has rarely been investigated. Hitchings [8] and Davis and Price [4] argue that this narrow perspective has produced security mechanisms that are, in practice, less effective than they are generally assumed to be. Since security mechanisms are designed, implemented, applied and breached by people, human factors should be considered in their design. It seems that currently, hackers pay more attention to the human link in the security chain than security designers do, for example, by using social engineering techniques to obtain passwords.

The key element in password security is the crackability of a password combination. Davies and Ganesan [3] argue that an adversary's ability to crack passwords is greater than usually believed. System-generated passwords are essentially the optimal security approach; however, user-generated passwords are potentially more memorable and thus less likely to be disclosed (because users do not have to write them down). The U.S. Federal Information Processing Standards [5] suggest several criteria for assuring different levels of password security. *Password composition*, for example, relates the size of a character set from which a password has been chosen to its level of security. An alphanumeric password is therefore more secure than one composed of letters alone. Short *password lifetime*—changing passwords frequently—is suggested as reducing the risk associated with undetected compromised passwords. Finally, *password ownership*, in particular individual ownership, is recommended to:

- Increase individual accountability;
- Reduce illicit usage;
- Allow for an establishment of system usage audit trails; and
- Reduce frequent password changes due to group membership fluctuations.

ANNE ADAMS AND MARTINA ANGELA SASSE

QUENTIN WEBB

A. Adams & M. A. Sasse (1999): **Users Are Not The Enemy: Why users compromise security mechanisms and how to take remedial measures,** in: Communications of the ACM, 42 (12), pp. 40-46 December 1999

Many security systems fail invisibly.

Which of these is encrypted?

U2FsdGVkX1/XlRf6Gt1czLSd9VgyKQatH76f4VFoF5w=

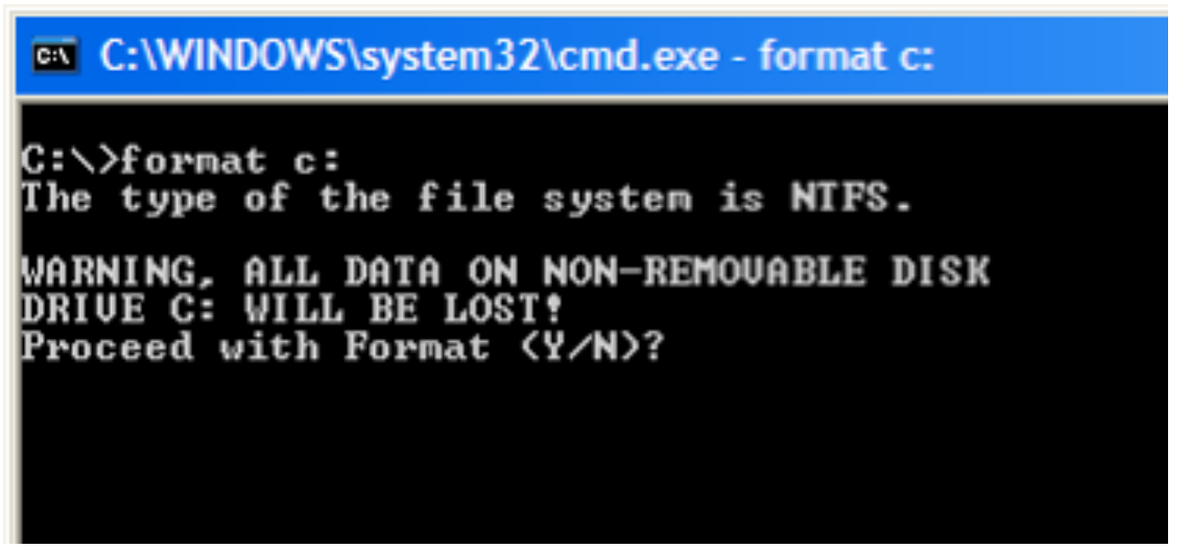
VGhpcyBpcyBhIHRlc3QK==

Which of these actually erases data?

format c: **(Windows 95)**

format c: **(Windows XP)**

format c: **(Vista)**



The lack of transparency makes it hard to understand online privacy & security.

Hidden Information at the Server:

- Log files
- Third-party Image Servers
- Web Bugs

Hidden Information at the Client:

- Cookies
- Browser History
- Browser Cache

DNS is opaque to most users:

- Many DNS names can map to one IP address
- Many IP addresses can map to one DNS name
- No relationship between a DNS name and a company

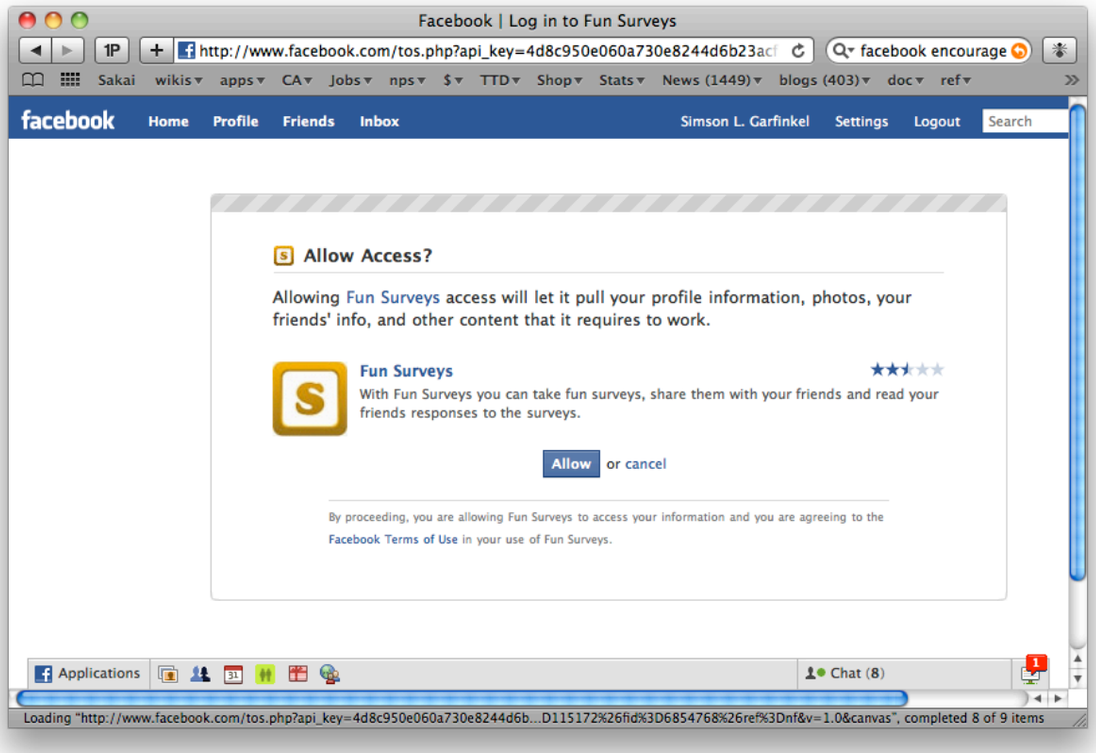
File-sharing programs and social networking websites encourage reckless sharing.

"A study of Kazaa P2P file Sharing," Good & Krekelberg,

- Lab study of users.
- Searched Kazaa for potentially confidential files.
- Made "Credit Cards.xls" file available; people tried to download it!

Facebook Applications (2009):

- Access all of your data
- Access your friend's data
- "Surveys" are applications.



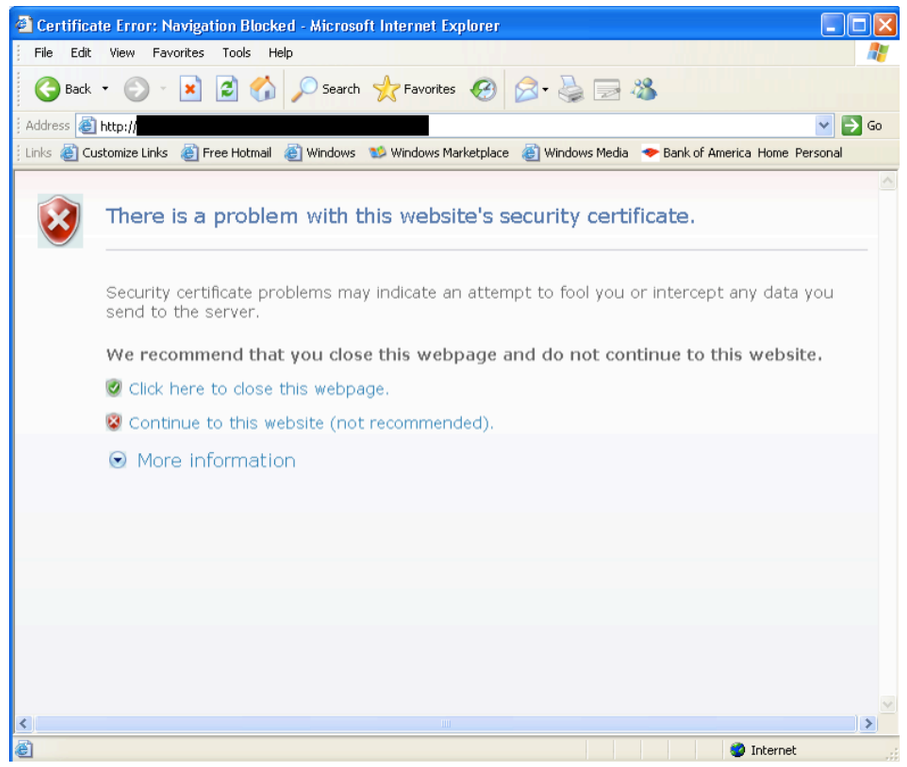
Users can't distinguish errors from attacks.

"The Emperor's New Security Indicators,"
Schechter, Dhamija, Ozment and Fischer, 2007

Study of Site Key.

- Study of 67 users under varying conditions.
- "https" removed
- site-authentication images remove ("site key not available at this time")
- SSL warning pages

23 of 25 participants (92%) provided username & password when Site Key authentication image was missing.

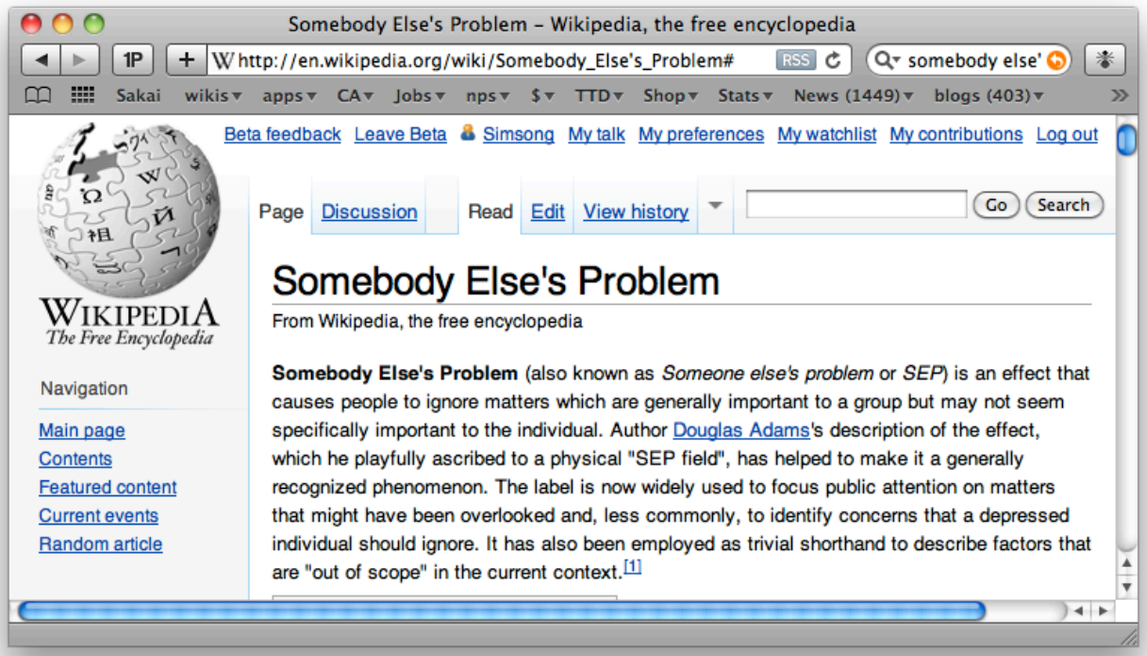


Users do not want to manage their security...

Users have real-world tasks

- Read email
- Prepare documents
- Get home and see the kids..

Managing security is a *secondary task* & somebody else's problem



The "Barn Door" property.

Once a secret is out, it's out.

http://www.crh.noaa.gov/Image/abr/06172007/pole_barn_west_door_damage.jpg

How do we design in "usable security" ?

There are three primary HCI-SEC approaches.

#1 — Make it "just work"

- Invisible security
- Fix the bugs!

#2 — Make security understandable

- Reduce configurability
- Visible security states
- Intuitive user interfaces
- Metaphors that users can understand

#3 — Train the user

Approach #1: Make it work

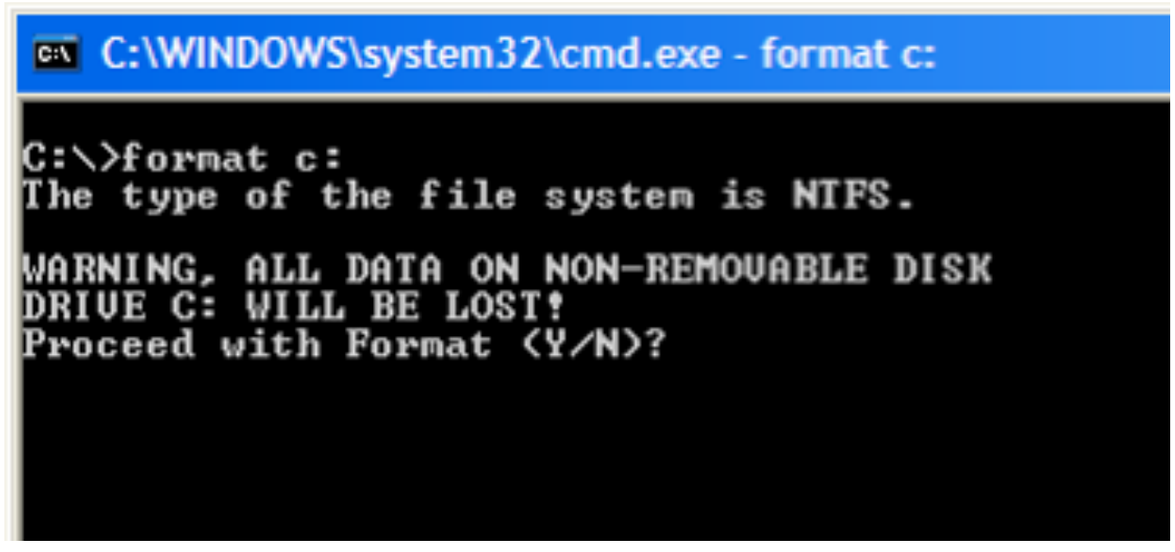
Example: Discarded Drives

- Between 1998 and 2007 I bought 1400 used drives.
- Most were "formatted"…
- … but most had recoverable information.

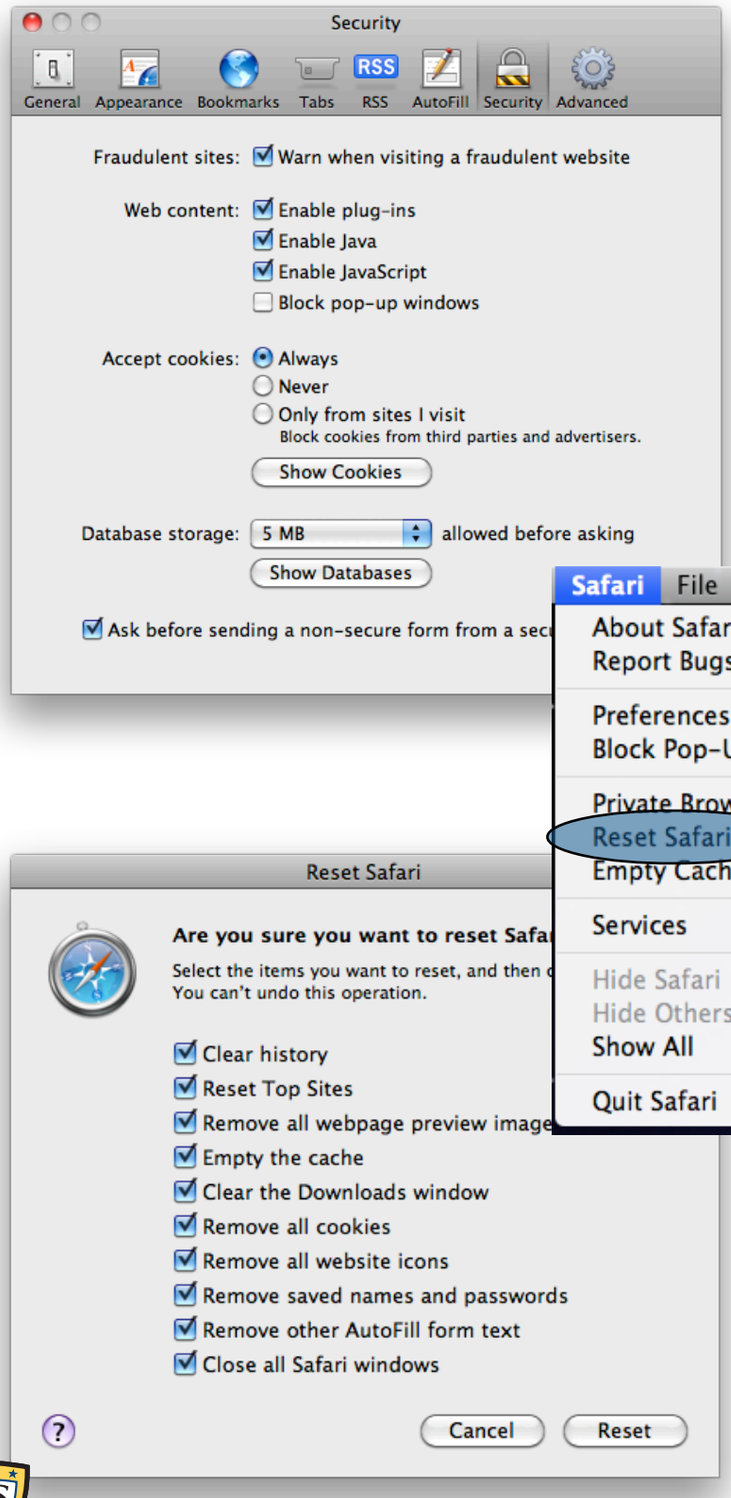
Solution: fix the "format" command

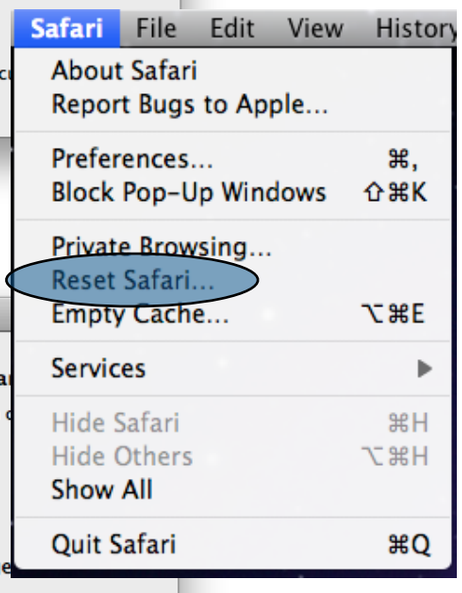
- In Windows 2003, format hides data.
- In Windows Vista, FORMAT erases data.

No longer a lie!

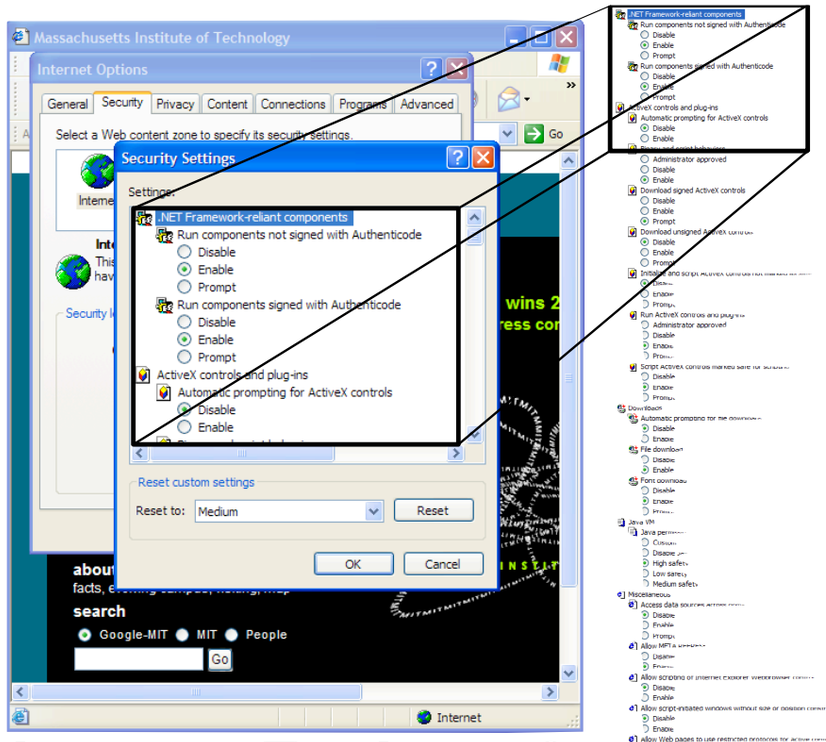


Approach #2: Make Security Understandable and Reduce configurability.





vs.

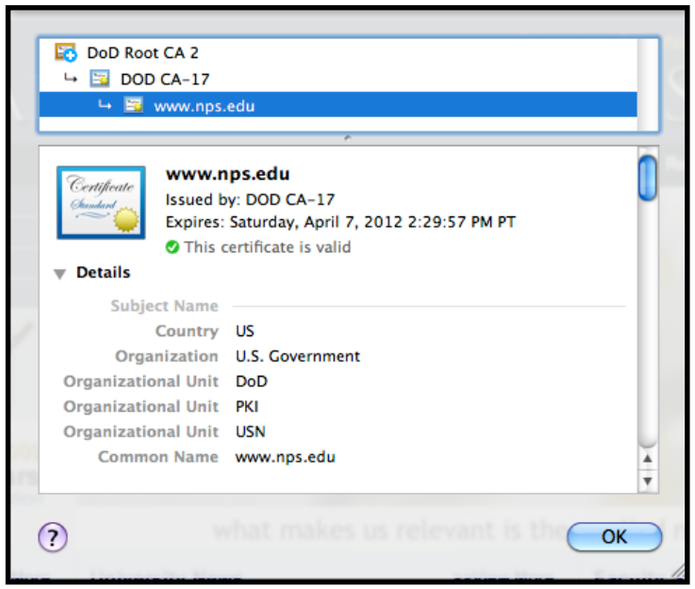


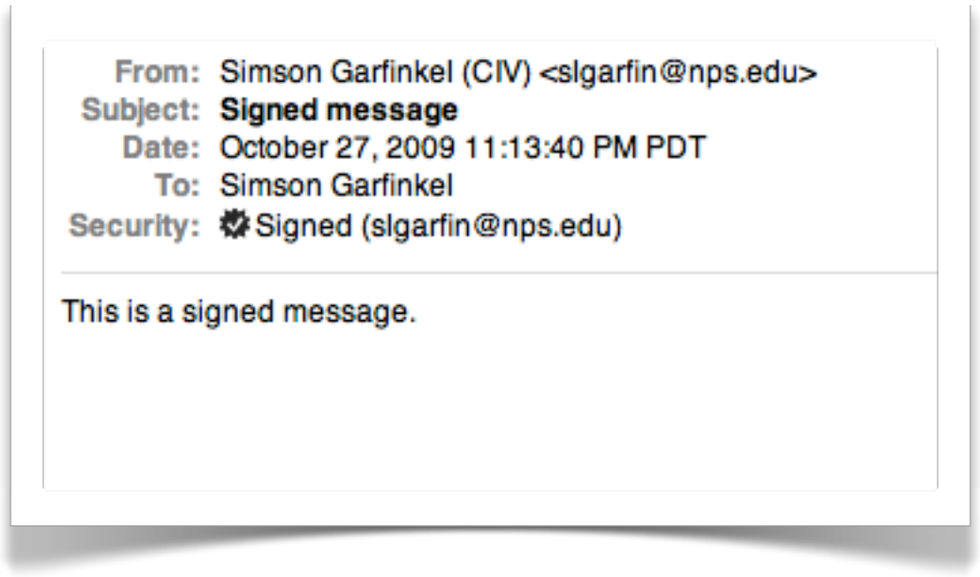
Internet Explorer 6

Approach #3: Train the user to act securely...

Give the user a consistent user experience.

- SSL certificates up-to-date
- Digitally signed mail





Give the user training consistent with their user experience.

NPS is actively researching HCI-SEC

Some Current Projects:

- Increased use of SSL; more attention to certificate validity.
- Signing of "Bulk Email"
- Biometric authentication and identity management.

Remember:

- "Those who would give up Essential **Usability** to purchase a little Temporary **Security**, deserve neither Usability nor Security."

— Benjamin Franklin
(sort of)